IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): B. M. Jakobsson et al.
Docket No.: 47-2
Serial No.: 10/060,599
Filing Date: January 30, 2002
Group: 2137
Examiner: Courtney D. Fields

Title: Method and Apparatus for Identification Tagging
Documents in a Computer System

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants (hereinafter "Appellants") hereby appeal the final rejection dated March 22, 2007 of claims 1-20 of the above-identified application.

REAL PARTY IN INTEREST

The present application is assigned of record to Lucent Technologies Inc. On November 30, 2006, the assignee Lucent Technologies Inc. completed a merger with Alcatel S.A., with the resulting entity being named Alcatel-Lucent. Alcatel-Lucent is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences.

STATUS OF CLAIMS

The present application was filed on January 30, 2002, with claims 1-20, all of which remain pending. Claims 1, 8 and 14 are the independent claims.

Each of claims 1-20 stands finally rejected under 35 U.S.C. §102(b). Claims 1-20 are appealed.

STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method for operation of a computer system for identification tagging a document created by said computer system and includes a step of calculating a function of the document. The method also includes a step of creating an identification tag by performing a cryptographic function on said function of the document and a unique processor identifier associated with said computer system, said cryptographic function producing an identification tag having the characteristics that a third party, said third party being unassociated with, and independent from, the creation of said created document by said computer system, possessing said document, said identification tag, and a plurality of unique processor associators each having a relationship to an associated one of a plurality of processor identifiers, can determine a source of said document as a function of identifying said computer system. The method further includes a step of attaching said identification tag to said document.

An illustrative embodiment of the method recited in claim 1 is described in the specification at, for example, page 5, line 32, to page 7, line 12, with reference to FIG. 3 in the drawings. In this illustrative embodiment, a method for operation of a computer system (e.g., computer 100 in FIG. 1) for identification tagging a document (e.g., that discussed in the present specification at page 5, lines 8-11) created by said computer system includes a step (e.g., 302 in FIG. 3) of calculating a function (e.g., hash value m) of the document. It also includes a step (e.g., 304 in FIG. 3) of creating an identification tag (e.g., that returned in step 306) by performing a cryptographic function on said function of the document and a unique processor

2

identifier (e.g., x_i 112 in FIG. 1) associated with said computer system, said cryptographic function producing an identification tag having the characteristics that a third party (e.g., that discussed in the specification at, for example, page 7, lines 12-18, in reference to FIG. 4), said third party being unassociated with, and independent from, the creation of said created document by said computer system, possessing (e.g., as discussed in the specification at, for example, page 7, lines 23-25) said document, said identification tag (e.g., that extracted in step 402 of FIG. 4), and a plurality of unique processor associators (e.g., 202 in FIG. 2) each having a relationship to an associated one of a plurality of processor identifiers (e.g., 112 in FIG. 1), can determine (e.g., step 414 of FIG. 4) a source of said document as a function of identifying said computer system. It further includes a step (e.g., 308 in FIG. 3) of attaching said identification tag to said document.

Independent claim 8 is directed to a processor including a stored unique processor identifier. The processor also includes stored tag function program code which when executed by the processor calculates an identification tag by performing a cryptographic function on a function of a document and said unique processor identifier, wherein said cryptographic function produces an identification tag having the characteristics that a third party, said third party being unassociated with, and independent from, the creation of said created document by said computer system, possessing said identification tag, said document, and a plurality of unique processor associators each having a relationship to an associated one of a plurality of processor identifiers, can identify a source of said creation of said document as a function of identifying said processor.

An illustrative embodiment of the processor recited in claim 8 is described in the specification at, for example, page 4, line 23, to page 5, line 5, with reference to FIG. 1 in the drawings. In this illustrative embodiment, a processor (e.g., 102) includes a stored unique processor identifier (e.g., x_i 112). The processor also includes stored tag function program code (e.g., 114) which when executed by the processor calculates (e.g., step 306 in FIG. 3) an identification tag by performing a cryptographic function (e.g., step 304 in FIG. 3) on a function (e.g., step 302 in FIG. 3) of a document and said unique processor identifier, wherein said cryptographic function produces an identification tag having the characteristics that a third party

3

(e.g., that discussed in the specification at, for example, page 7, lines 12-18, in reference to FIG. 4), said third party being unassociated with, and independent from, the creation of said created document by said computer system, possessing (e.g., as discussed in the specification at, for example, page 7, lines 23-25) said identification tag (e.g., that extracted in step 402 of FIG. 4), said document, and a plurality of unique processor associators (e.g., 202 in FIG. 2) each having a relationship to an associated one of a plurality of processor identifiers (e.g., 112 in FIG. 1), can identify (e.g., step 414 of FIG. 4) a source of said creation of said document as a function of identifying said processor.

Independent claim 14 is directed to a computer system for identification tagging a document created by said computer system including means for calculating a function of the document. The computer system also includes means for creating an identification tag by performing a cryptographic function on said function of the document and a unique processor identifier associated with said computer system, said cryptographic function producing an identification tag having the characteristics that a third party, said third party being unassociated with, and independent from, the creation of said created document by said computer system, possessing said document, said identification tag, and a plurality of unique processor associators each having a relationship to an associated one of a plurality of processor identifiers, can determine a source of said document as a function of identifying said computer system which created said document. The computer system further includes means for attaching said identification tag to said document.

An illustrative embodiment of the computer system recited in claim 14 is described in the specification at, for example, page 5, line 32, to page 7, line 12, with reference to FIGS. 1 and 3 in the drawings. In this illustrative embodiment, a computer system (e.g., 100 in FIG. 1) for identification tagging a document created by said computer system including means (e.g., processor 102 executing a computer program code stored directly on processor 102, in random access memory 104, in non-volatile memory 106, or in any other memory to which processor 102 has access, discussed in the specification at, for example, page 5, line 32, to page 6, line 3) for calculating (e.g., step 302 in FIG. 1) a function (e.g., hash value m) of the document. The computer system also includes means (e.g., processor 102 executing a computer program code

stored directly on processor 102, in random access memory 104, in non-volatile memory 106, or in any other memory to which processor 102 has access, discussed in the specification at, for example, page 5, line 32, to page 6, line 3) for creating (e.g., 304 in FIG. 3) an identification tag (e.g., that returned in step 306) by performing a cryptographic function on said function of the document and a unique processor identifier (e.g., x_i 112 in FIG. 1) associated with said computer system, said cryptographic function producing an identification tag having the characteristics that a third party (e.g., that discussed in the specification at, for example, page 7, lines 12-18, in reference to FIG. 4), said third party being unassociated with, and independent from, the creation of said created document by said computer system, possessing (e.g., as discussed in the specification at, for example, page 7, lines 23-25) said document, said identification tag (e.g., that extracted in step 402 of FIG. 4), and a plurality of unique processor associators (e.g., 202 in FIG. 2) each having a relationship to an associated one of a plurality of processor identifiers (e.g., 112 in FIG. 1), can determine (e.g., step 414 of FIG. 4) a source of said document as a function of identifying said computer system. The computer system further includes means (e.g., processor 102 executing a computer program code stored directly on processor 102, in random access memory 104, in non-volatile memory 106, or in any other memory to which processor 102 has access, discussed in the specification at, for example, page 5, line 32, to page 6, line 3) for attaching (e.g., 308 in FIG. 3) said identification tag to said document.

The claimed invention provides a number of significant advantages over conventional arrangements. For example, as discussed in the specification at page 1, line 27, to page 2, line 26, unlike conventional techniques, the claimed invention provides a method and apparatus that allows for the investigative tracing of computer generated documents while preventing unauthorized third parties from determining the identity of other users and from framing other users. Further advantages associated with embodiments of the claimed invention are discussed in the specification at, for example, page 3, lines 3-22, and page 10, lines 6-31.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-20 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 6,418,472 (hereinafter "Mi").

ARGUMENT

Appellants incorporate by reference herein the disclosure of their previous responses filed in the present application, including the responses dated January 8, 2007, and June 22, 2007.

§102(b) Rejection of Claims 1-20 over Mi

Claims 1, 3, 5, 7, 8, 10, 12, 14, 16, 18 and 20

Appellants initially note that MPEP §2131 specifies that a given claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Appellants respectfully traverse the §102(b) rejection on the ground that the Mi reference fails to teach or suggest each and every limitation of claims 1-20 as alleged. For example, the method of independent claim 1 recites steps of "calculating a function of the document" and "creating an identification tag by performing a cryptographic function on said function of the document and a unique processor identifier." In an illustrative embodiment described with reference to steps 302 and 304 of FIG. 3 at page 6, lines 5-33, the document to be tagged is first hashed to determine a hash value. Then, the tag function is called, passing it the hash value as a parameter, and performs a cryptographic function on both the hash value and a unique processor identifier.

In the final Office Action, the Examiner alternatively contends that the recited limitation directed to calculating a function of the document is taught by Mi at column 3, lines 7-16 (see the last full paragraph of page 3 of the final Office Action) and at column 7, lines 1-14 (see the last paragraph of page 2 of the final Office Action). Appellants respectfully submit that neither of these cited portions of Mi teaches or suggests this limitation.

6

Rather, column 3, lines 7-16, of Mi discloses a technique wherein a module "can access information embedded in a processor, e.g., a processor number, and calculate from that embedded information a value that may be compared with processor identifier. . . ." This portion of Mi does not mention any document, much less disclose calculating a function of a document based at least in part on at least a portion of the contents of the document.

Similarly, column 7, lines 1-14, of Mi discloses:

> If object 401 is a patient's medical record, for example, and that patient has a computer or other device that can access web site 402, server 400 may store a processor identifier 403 corresponding to that computer or device when storing that medical record. Processor identifier 403 may be the computer's processor number or a value resulting from applying a function to the combination of that processor number and a value associated with web server 400, such as server identifier 406. To register a client computer for permitted access to object 401, such as the patient's computer described above, server 400 can generate a hash value calculated from the combination of the computer's processor number and server identifier 406. Server 400 can then store the resulting hash value as processor identifier 403 (block 505).

This portion of Mi likewise fails to disclose steps of "calculating a function of the document" and "creating an identification tag by performing a cryptographic function on said function of the document and a unique processor identifier." Rather, it teaches away by disclosing an alternative technique wherein a server stores a value calculated from the combination of a computer's processor number and a server identifier associated with a web server. Appellants respectfully submit that, despite the Examiner's apparent contention that this section teaches calculating a function of a document because "the document is assigned a processor identifier," neither processor identifier 403 ("corresponding to that computer" used by a patient to access a web site) nor server identifier 406 ("associated with web server") is a function of object 401.

In the Advisory Action dated July 11, 2007, the Examiner contends that "Mi et al. discloses the means for calculating a function (i.e., hash) of a document in Column 7, lines 1-14) [sic] As clearly shown, the document is a patient's medical record which is stored upon a computer, the document is assigned a processor identifier which is unique to the patient's

medical record." As discussed above, Appellants respectfully submit that Mi discloses neither calculating a hash of a patient record nor a processor identifier unique to, or even based on, the patient's medical record. As the Examiner correctly concedes in the Advisory Action, Mi's "hash value is generated and calculated from the combination of the processor number and the value associated with the server identifier;" neither of these values are related to a document.

In the Advisory Action, the Examiner also argues that "Mi et al. further discloses another embodiment wherein a verification agent obtains a secret key. The cryptographic function is performed wherein a return value is calculated using embedded information, a secret key, and a session identifier. (See Column 4, lines 24-34)." Here again, Mi fails to teach or suggest steps of "calculating a function of the document" and "creating an identification tag by performing a cryptographic function on said function of the document and a unique processor identifier."

Rather, the relied-upon portion of Mi teaches the calculation of "a return value that is a function of embedded information 211, secret key 214, and session identifier 213." Mi, at column 3, lines 42-62, teaches that embedded information 211 is a value which identifies processor 210, e.g., a processor number. Mi at column 4, lines 21 and 34-38 teaches that secret key 214 is unique to, and included in, the verification agent and, moreover, that the secret key may a random number generated using a random number generator. Likewise, Mi, at column 4, lines 3-8, discloses, with emphasis added, that session identifier 213, which may comprise a randomly generated number, "provides a means for matching a value returned from a client computer 200 with a specific attempt to access object 202," rather than being a function of a document. Thus, this section of Mi also fails to anticipate the aforementioned limitation.

Furthermore, claim 1 recites a limitation wherein "a third party, said third party being unassociated with, and independent from, the creation of said created document by said computer system, possessing said document, said identification tag, and a plurality of unique processor associators each having a relationship to an associated one of a plurality of processor identifiers, can determine a source of said document as a function of said computer system." An illustrative embodiment is described with reference to FIG. 4 in the present specification at, for example, page 7, lines 13-31, wherein it may be "known that the user identified by the user

identification data associated with the particular processor associator . . . is the source of the document."

The techniques disclosed in Mi fail to teach or suggest <u>determining a source</u> of a document based at least in part on an identification tag attached to the document. Rather, Mi discloses only techniques for verifying the identity of a platform seeking <u>access</u> to an object. See Mi at, for example, column 1, lines 1-11, and column 11, line 66, to column 12, line 1.

Accordingly, it is believed that the teachings of Mi fail to anticipate the limitations of independent claim 1.

Independent claims 8 and 14 contain limitations similar to those of independent claim 1 and are believed patentable for at least the reasons identified above in reference to claim 1.

Dependent claims 3, 5, 7, 10, 12, 16, 18 and 20 are believed allowable for at least the reasons identified above with regard to the independent claims from which they depend.

<u>Claims 2, 9 and 15</u>

Dependent claims 2, 9 and 15 are believed allowable for at least the reasons identified above with regard to the independent claims from which they depend. Additionally, these claims define separately patentable subject matter.

More specifically, claims 2, 9 and 15 recite similar limitations "wherein said function of the document is a hash function." In formulating the rejection of these claims in the final Office Action, the Examiner relies on column 4, lines 24-34, of Mi, which teaches that "in the case where verification agent 212 includes another value, e.g., a server identifier, in addition to secret key 214, calculator 215 may employ a hash function, such as SHA-1 or MD5, to calculate a return value that is a function of embedded information 211, secret key 214, session identifier 213 and that additional value." Appellants respectfully submit that Mi's disclosure wherein a hash function is employed to calculate a return value that is a function of information embedded in a processor, a secret key, a session identifier, and another value included in a verification agent, such as a server identifier, fails to anticipate the recited limitation wherein a <u>function of the document</u> is a hash function.

Claims 4, 11 and 17

Dependent claims 4, 11 and 17 are believed allowable for at least the reasons identified above with regard to the independent claims from which they depend. Additionally, these claims define separately patentable subject matter.

More specifically, claims 4, 11 and 17 recite similar limitations "wherein said cryptographic function is a Message Authentication Code." In formulating the rejection of these claims in the final Office Action, the Examiner relies upon column 2, lines 53-58, of Mi, which discloses that an object may consist of data and/or executable code and may be stored in a machine readable storage medium. Appellants respectfully submit that such disclosures are inapposite to the recited limitation. Indeed, Mi fails to mention a Message Authentication Code at all, much less disclose its use in the claimed manner.
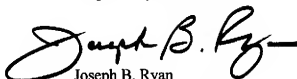
Claims 6, 13 and 19

Dependent claims 6, 13 and 19 are believed allowable for at least the reasons identified above with regard to the independent claims from which they depend. Additionally, these claims define separately patentable subject matter.

More specifically, claims 6, 13 and 19 recite similar limitations "wherein said cryptographic function is based on modular exponentiation." In formulating the rejection of these claims in the final Office Action, the Examiner relies upon column 8, lines 33-46, of Mi, which discloses techniques directed toward calculating and sending a hash value. Appellants submit that these disclosures fail to teach or suggest the recited limitation wherein a cryptographic function is based on modular exponentiation.

In view of the above, Appellants believe that claims 1-20 are in condition for allowance, and respectfully request the withdrawal of the §102(b) rejections.

Respectfully submitted,

Date: September 24, 2007

Joseph B. Ryan
Attorney for Appellant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

CLAIMS APPENDIX

1. A method for operation of a computer system for identification tagging a document created by said computer system comprising the steps of:

calculating a function of the document;

creating an identification tag by performing a cryptographic function on said function of the document and a unique processor identifier associated with said computer system, said cryptographic function producing an identification tag having the characteristics that a third party, said third party being unassociated with, and independent from, the creation of said created document by said computer system, possessing said document, said identification tag, and a plurality of unique processor associators each having a relationship to an associated one of a plurality of processor identifiers, can determine a source of said document as a function of identifying said computer system; and

attaching said identification tag to said document.

2. The method of claim 1 wherein said function of the document is a hash function.

3. The method of claim 1 wherein said relationship between a unique processor identifier and its associated unique processor associator is one of equality.

4. The method of claim 3 wherein said cryptographic function is a Message Authentication Code.

5. The method of claim 1 wherein said relationship between a unique processor identifier and its associated unique processor associator is that said unique processor identifier is a function of its associated processor associator.

6. The method of claim 5 wherein said cryptographic function is based on modular exponentiation.

7. The method of claim 1 wherein said unique processor identifier is stored in a processor of said computer system.

8. A processor comprising:

a stored unique processor identifier; and

stored tag function program code which when executed by the processor calculates an identification tag by performing a cryptographic function on a function of a document and said unique processor identifier, wherein said cryptographic function produces an identification tag having the characteristics that a third party, said third party being unassociated with, and independent from, the creation of said created document by said computer system, possessing said identification tag, said document, and a plurality of unique processor associators each having a relationship to an associated one of a plurality of processor identifiers, can identify a source of said creation of said document as a function of identifying said processor.

9. The processor of claim 8 wherein said function of a document is a hash function.

10. The processor of claim 8 wherein said relationship between a unique processor identifier and its associated unique processor associator is one of equality.

11. The processor of claim 10 wherein said cryptographic function is a Message Authentication Code.

12. The processor of claim 8 wherein said relationship between a unique processor identifier and its associated unique processor associator is that said unique processor identifier is a function of its associated processor associator.

13. The processor of claim 12 wherein said cryptographic function is based on modular exponentiation.

14. A computer system for identification tagging a document created by said computer system comprising:

means for calculating a function of the document;

means for creating an identification tag by performing a cryptographic function on said function of the document and a unique processor identifier associated with said computer system, said cryptographic function producing an identification tag having the characteristics that a third

party, said third party being unassociated with, and independent from, the creation of said created document by said computer system, possessing said document, said identification tag, and a plurality of unique processor associators each having a relationship to an associated one of a plurality of processor identifiers, can determine a source of said document as a function of identifying said computer system which created said document; and

      means for attaching said identification tag to said document.

15. The computer system of claim 14 wherein said function of the document is a hash function.

16. The computer system of claim 14 wherein said relationship between a unique processor identifier and its associated unique processor associator is one of equality.

17. The computer system of claim 16 wherein said cryptographic function is Message Authentication Code.

18. The computer system of claim 14 wherein said relationship between a unique processor identifier and its associated unique processor associator is that said unique processor identifier is a function of its associated processor associator.

19. The computer system of claim 18 wherein said cryptographic function is based on modular exponentiation.

20. The computer system of claim 14 wherein said unique processor identifier is stored in a processor of said computer system.

EVIDENCE APPENDIX

None

<u>RELATED PROCEEDINGS APPENDIX</u>

None